## REMARKS

Favorable reconsideration of the application is respectfully requested in light of the amendments and remarks herein.

Upon entry of this amendment, claims 1-19 will be pending. By this amendment, claims 1 and 11 have been amended. No new matter has been added.

§ 102 Rejection of Claims 1-5, 8-14, and 17-19

In Section 2 of the Office Action, claims 1-5, 8-14, and 17-19 stand rejected under 35 U.S.C. §102(b) as being unpatentable over Seth-Smith *et al.* (U.S. Patent 4,829,569; hereinafter referred to as "Seth-Smith"). Claims 1 and 11 have been amended to address the rejection.

In the Background section of the Specification, it was disclosed that "if a data transmission network is structured using satellite links, one network can cover an area wider than the whole country such as Japan. On such a network, data transmitted to a data receiver on the northernmost island of Hokkaido can be tapped by a data receiver in the southernmost Okinawa Prefecture. That is, on any satellite link-based network to which a large number of data receivers are configured, there is an increased possibility of data being illicitly tapped by unintended parties. [However, in] a data transmission setup utilizing broadcast type communication channels such as satellite links, untreated data can be received not only by the intended data receiver but also by those not supposed to receive the data in question. One solution to this problem with today's digital data broadcasting systems using a communication satellite is the encryption of data (i.e., primarily video and audio information) prior to their transmission over satellite communication links." *Specification, page 5, lines 4-22.*

"The following problems have been generally experienced in connection with television broadcasts utilizing satellite links: A first problem is the limited number of authorized data receivers . . . . A second problem is the increase in costs on the transmitting side in keeping with a growing number of PIDs in use . . . . A third problem is the inability of the data transmitter in one-way data transmission over satellite links to know whether information has been correctly transmitted to destination data receivers . . . . A fourth problem concerns a poor affinity with the Internet Protocol when an IP datagram must be transmitted with its PID adjusted to an IP destination address by the data transmitter . . . . A fifth problem is that the need for each application to be provided with its own controlling method makes prompt handling of newly introduced applications difficult . . . . A sixth problem is that while the authentication header and encapsulating security payload are application-independent, there are virtually no network devices compatible with these methods at the level of the current version of the Internet Protocol (e.g., IP v4)." *Page 9, line 24 to page 11, line 21 of the Specification.*

To solve the above-described problems, embodiments of the present invention provide system and method for controlling transmission of data from data transmitting means to data receiving means over at least first and second communication channels. For example, the steps of a data transmission controlling method of claim 1, as presented herein, includes:

> "*transmitting data encrypted by said data transmitting means* to said data receiving means over a first communication channel provided for data transmission from said data transmitting means to said data receiving means,
>
> *wherein* prior to transmitting said encrypted data over said first communication channel, said data transmitting means encapsulates data to be transmitted from said data transmitting means to data receiving means in accordance with a plurality of protocols,
>
> *wherein* at least one of said data capsules resulting from the encapsulation is encrypted, and

> *wherein* said data transmitting means supplements an encrypted data section with a section header containing destination address information; and
>
> *transmitting restrictive data transmission control information* to said data receiving means over a second communication channel having a smaller capacity of data transmission than said first communication channel,
>
> *wherein* said restrictive data transmission control information transmitted over said second communication channel is operating to allow only intended data receiving means to receive the encrypted data, and is configured to substantially simplify decryption of the encrypted data transmitted over said first communication channel."

(emphasis added)

Therefore, the data transmission controlling method of claim 1 controls transmission of data from data transmitting means to data receiving means over at least a first and second communication channel, wherein prior to transmitting encrypted data over said first communication channel, said data transmitting means encapsulates data to be transmitted from said data transmitting means to data receiving means in accordance with a plurality of protocols, wherein at least one of said data capsules resulting from the encapsulation is encrypted *(Specification, page 15, lines 8-14; pages 25-27)*, and wherein said data transmitting means supplements an encrypted data section with a section header containing destination address information *(Specification, page 27, lines 5-7 and 16-17)*. Further, the restrictive data transmission control information transmitted over the second communication channel is operating to allow only intended data receiving means to receive the encrypted data, and is configured to substantially simplify decryption of the encrypted data transmitted over the first communication channel.

Seth-Smith cited for teaching that "the restrictive data transmission control information transmitted over the second communication channel operates to allow only intended data receiving means to receive the encrypted data, and is configured to substantially simplify decryption of the encrypted data transmitted over the first communication channel." *Office Action, part 3, pages 2-3.* Yet the cited section of Seth-Smith does not discuss simplifying decryption of encrypted data. For example, the cited lines of Seth-Smith disclose the object of the invention is to provide a subscription television system in which text messages can be transmitted . . . in which the message can only be received by the proper receiver . . . and is heavily protected against improper receipt . . . ." *Seth-Smith, col. 3, lines 14-22.* Further, an encrypted signal "is transmitted . . . via a satellite 20, by a landline or a combination of both to receiving antenna 22," passed to a decoder which detects the signal, decrypts portions of it, completes messages requiring information such as billing status information and the like, and displays received messages. *Seth-Smith, col. 6, lines 47-65.* These passages fail to mention, teach or suggest configuring restrictive data control transmission information to simplify decryption of encrypted data transmitted over the first communication channel, as claimed.

Further, Seth-Smith fails to teach or suggest a method *wherein* prior to transmitting encrypted data over said first communication channel, said data transmitting means encapsulates data to be transmitted from said data transmitting means to data receiving means in accordance with a plurality of protocols, *wherein* at least one of said data capsules resulting from the encapsulation is encrypted, and *wherein* said data transmitting means supplements an encrypted data section with a section header containing destination address information. These features further the invention's objective of solving the second, fifth and sixth problems with the prior art as described earlier. *See Specification, pages 28-30.*

Therefore, Seth-Smith fails to teach or suggest controlling transmission of data from data transmitting means to data receiving means over at least first and second communication channels, *wherein* prior to transmitting encrypted data over said first communication channel, said data transmitting means encapsulates data to be transmitted from said data transmitting means to data receiving means in accordance with a plurality of protocols, *wherein* at least one of said data capsules resulting from the encapsulation is encrypted, and *wherein* said data transmitting means supplements an encrypted data section with a section header containing destination address information; and wherein restrictive data transmission control information transmitted over the second communication channel is operating to allow only intended data receiving means to receive the encrypted data, and is configured to substantially simplify decryption of the encrypted data transmitted over the first communication channel.

Based on the foregoing discussion, it is maintained that Seth-Smith fails to disclose, teach or suggest all the limitations recited in claim 1. Therefore, claim 1 should be allowable over Seth-Smith. Since claim 11 closely parallels, and includes substantially similar limitations as recited in, claim 1, claim 11 should also be allowable over Seth-Smith. Further, since claims 2-5 and 8-10 depend from claim 1, and claims 12-14 and 17-19 depend from claim 11, claims 2-5, 8-10, 12-14, and 17-19 should be allowable over Seth-Smith.

Accordingly, it is submitted that the rejection of claims 1-5, 8-14, and 17-19 based upon 35 U.S.C. §102(b) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§ 103 Rejection of Claims 6-7 and 15-16

In Section 11 of the Office Action, claims 6-7 and 15-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Seth-Smith in view of Mueller (U.S. Patent 5,602,917).

Based on the foregoing discussion regarding claims 1 and 11, and since claims 6-7 and

15-16 depend from claims 1 and 11, respectively, claims 6-7 and 15-16 should be allowable over Seth-Smith. Further, Mueller is merely cited for disclosing a master key that encrypts and decrypts session keys. Therefore, claims 6-7 and 15-16 should be allowable over Seth-Smith and Mueller.

Accordingly, it is submitted that the rejection of claims 6-7 and 15-16 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Conclusion

In view of the foregoing, entry of this amendment, and the allowance of this application with claims 1-19 are respectfully solicited.

In regard to the claims amended herein and throughout the prosecution of this application, it is submitted that these claims, as originally presented, are patentably distinct over the prior art of record, and that these claims were in full compliance with the requirements of 35 U.S.C. §112. Changes that have been made to these claims were not made for the purpose of patentability within the meaning of 35 U.S.C. §§101, 102, 103 or 112. Rather, these changes were made simply for clarification and to round out the scope of protection to which Applicant is entitled.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number written below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP

By: Samuel S. Lee, Reg. No. 42,791 for
William S. Frommer
Reg. No. 25,506
(212) 588-0800